CLAIMS:

1. A method for automated adaptive reprovisioning of servers under security assault, the method comprising:

detecting a security assault or a possible security assault on a first server; and

reprovisioning by automatically creating a new server instance with a desired new server configuration to perform at least one of the tasks performed by said first server.

2. The method of claim 1, wherein said detecting comprises determining if said first server is a candidate for reprovisioning, because of properties or behavior that suggest its security has been compromised or is likely to be compromised, or its functioning otherwise unacceptably impaired, by a security assault.

3. The method of claim 1, wherein said reprovisioning comprises automatically bringing up said new server instance, or otherwise making available said new server instance to customers or other users of said first server.

4. The method of claim 1, further comprising bringing down said first server prior to said reprovisioning.

5. The method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server in at least one parameter.

6. The method of claim 1, wherein a difference between said new server instance and said first server is responsive to whether or not other security incidents have been detected in a network to which said servers are coupled.

7. The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a nature of any other security incidents that have been detected in said network to which said servers are coupled.

8. The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a probable compromise or a functional impairment observed in said detection.

9. The method of claim 1, wherein a difference between said new server instance and said first server includes a version of server software used by said servers.

10. The method of claim 1, wherein a difference between said new server instance and said first server includes a version of operating system software used by said servers.

11. The method of claim 1, wherein a difference between said new server instance and said first server includes a version of network connectivity software used by said servers.

12. The method of claim 1, wherein a difference between said new server instance and said first server includes strength of encryption used by said servers.

13. The method of claim 1, wherein a difference between said new server instance and said first server includes a degree of function offered to users by said servers.

14. The method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server only if more than a fixed number of instances of probable server compromise have been observed.

15. The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a number of probable server compromises that have been observed.

16. The method of claim 1, wherein said server comprises a computer providing services through a network.

17. The method of claim 1, wherein said server comprises a program running on a network-coupled computer, providing services through a network.

18. The method of claim 1, wherein said reprovisioning comprises selecting said desired new server configuration for said new server instance from a plurality of new server configurations.

19. The method of claim 18, wherein said selecting said desired new server configuration for said new server instance comprises selecting a new server configuration from a table of new server configurations.

20. The method of claim 18, wherein said selecting said desired new server configuration for said new server instance comprises randomly selecting a new server configuration from among all new server configurations in a table.

21. The method of claim 18, wherein said selecting said desired new server configuration for said new server instance comprises randomly selecting a new server configuration from among all new server configurations in a table for which no probable compromise has been observed.

22. The method of claim 18, wherein said selecting said desired new server configuration for said new server instance comprises indexing into a table according to a number of times a server providing a function of said first server has been subject to probable compromise.

23. A computer-readable medium having stored thereon a plurality of instructions for automated adaptive reprovisioning of servers under security assault, said plurality of instructions including instructions which, when executed by a processor, cause said processor to perform:

detecting a security assault or a possible security assault on a first server; and

reprovisioning by automatically creating a new server instance with a desired new server configuration to perform at least one of the tasks performed by said first server.

24. The computer-readable medium of claim 23, wherein said detecting comprises determining if said first server is a candidate for reprovisioning, because of properties or behavior that suggest its security has been compromised or is likely to be compromised, or its functioning otherwise unacceptably impaired, by a security assault.

25. The computer-readable medium of claim 23, wherein said reprovisioning comprises automatically bringing up said new server instance, or otherwise making available said new server instance to customers or other users of said first server.

26. The computer-readable medium of claim 23, further comprising bringing down said first server prior to said reprovisioning.

27. The computer-readable medium of claim 23, wherein said new server instance brought up in said reprovisioning differs from said first server in at least one parameter.

28. The computer-readable medium of claim 23, wherein a difference between said new server instance and said first server is responsive to whether or not other security incidents have been detected in a network to which said servers are coupled.

29. The computer-readable medium of claim 23, wherein a difference between said new server instance and said first server is responsive to a nature of any other security incidents that have been detected in said network to which said servers are coupled.

30. A system for automated adaptive reprovisioning of servers under security assault, the system comprising:

a first server;

a security monitor, coupled to said first server, for detecting if said first server is a candidate for automatic reprovisioning with a new server instance; and

a provisioner, coupled to said first server, for automatically reprovisioning said server with said new server instance if said server is such a candidate.